THE GROWING MENACE OF IDENTITY THEFT TO NEW YORK CONSUMERS

by US Senator Charles E. Schumer

Identity theft is running rampant throughout New York and, with the holiday shopping season now underway, the problem promises to grow even more menacing to area consumers. This report is intended to detail the scope of identity theft across New York State and its impact on consumers; what New Yorkers need to do to protect themselves from identity theft and several proposals for the FTC to implement in order to prevent identity theft:

THE SCOPE OF THE PROBLEM AND ITS IMPACT

- In New York State, there were over 7,000 identity theft victims in 2001 and over 3,300 identity fraud cases in New York City.

- New York City had more identity theft than any other US city in 2001. It had more than twice the number of identity theft cases than Chicago, which had the second highest number of cases in the country with 1,470.

- After California, New York State had the second highest number of cases of any state in the nation or almost 10% of the identity theft cases in the country last year. Nationwide, there were 86,168 identity thefts in 2001, 36,020 of which were credit card fraud.

New York Cities with the Most Identity Theft

City	Number of Victims
New York City	3,315
Rochester	116
Buffalo	93
Yonkers	53
Albany	38

- 27,000 New York City residents and 60,000 New Yorkers statewide could be hit by identity theft on an annual basis by 2006, according to Schumer. Nationwide, between 500,000 and 700,000 people annually are expected to be victims of identity theft by 2006.

- Identity theft made up 42 percent of the consumer complaints filed with the FTC last year, making it the top source of consumer complaints in 2001.

- Identity theft is the most popular form of consumer fraud, in part because it is the most profitable. Identity thieves stole nearly $100 million from financial institutions last year, or an average of $6,767 per victim. It costs the average victim more than $1,000 to cope with the damage from identity theft.

IDENTITY THEFT AND ITS MOST COMMON FORMS IN NEW YORK

Identity theft occurs when the thief uses another person's name and social security number without prior consent to apply for services requiring a credit check. The perpetrator will register for the services and have all billing information sent to a fake address so that the victim has no idea that his identity has been stolen. The thief then uses the services without paying for them, ruining the victim's credit rating as agencies seek to collect unpaid debt. *The most common forms of identity theft in New York involve two types of credit card fraud and wireless fraud, accounting for almost 60% of all identity theft in the State in 2001:*

Most Common Types of Identity Theft in New York State

Type	Number of Victims
Credit Card Fraud	3,461
Phone or Utilities Fraud	1,612
Bank Fraud	580
Loan Fraud	490
Govt Document and Benefits Fraud	363

- ***Credit card fraud*** occurs when an identity thief intercepts mailings sent to an individual offering a new credit card and then uses those mailings to open a new account. The thief uses the victim's social security number and name to apply for the card while changing the billing address, and then uses the card and fails to pay the bills, leaving the victim to deal with collection agencies. In 2001, 31 percent of all identity theft cases in New York State involved this kind of fraud.

  An identity thief may also take advantage of existing credit card accounts by using store receipts to track down names and card numbers of victims that are in turn used to make purchases online or in stores. Account holders are then left to dispute the charges with their credit card companies. Almost 14 percent of all identity theft in New York occurred in this manner in 2001.

- ***Wireless fraud*** occurs when an identity thief uses a victim's name and social security number to apply for a mobile phone contract. After passing the credit check, the thief uses a billing address different from the victim's to ensure the victim remains unaware of the theft. The thief then uses the phone until the contract is cancelled due to lack of payment.

The victim only discovers the fraud when collection agencies seek to recover the thief's accumulated unpaid bills and inform the victim of their now damaged credit rating. Over 15 percent of all identity theft in New York State in 2001 occurred in this way.

SOLUTIONS

The following are several measures the FTC should look into implementing:

- Increase the Security of Credit Databases: Companies that access credit histories should use background checks to ensure that their employees do not have criminal records through background checks. Since a person's privacy data is usually held by multiple credit agencies, the companies that provide access to credit histories should all be subject to the same security standards to ensure that security at one agency is not worse than that at another.

- Limit Access to Credit Information: Those accessing credit histories should be able to do so only on a "need-to" basis. Currently, anyone with access to credit histories at a credit agency can access any record in the database even if they have no official need to do so.

- Require New Credit Account Notification: Credit reporting agencies should notify a consumer when a new credit account is opened in his or her name. This would also alert the customer to a possible identity theft in progress. Banks, for example, already take these kinds of precautionary steps when address changes are made on accounts, sending notification to both the old and new address of the bank account holder to allow the holder to confirm that the change was indeed requested.

- Truncate Credit Card Receipts: Credit card receipts and credit card statements should not list the full credit card numbers. Many ATM receipts list truncated numbers to prevent access to the accounts by unauthorized persons. This simple change would dramatically curtail the ability of identity thieves to commit credit card fraud. Although some companies and stores already do this (Visa and MasterCard, for example, require that truncation be done at certain public venues, like gas stations, but do not require it to be done everywhere), the practice is not universal. The industry could save millions since truncation would reduce fraud.

- Streamline the Process for Identity Theft Victims to Restore Their Credit Rating: Since credit companies have different standards for erasing erroneous information form credit histories, identity theft victims often have a difficult time trying to erase the black marks from their credit histories caused by the perpetrators. The FTC should develop a single standard of proof in cases of ID theft to streamline the recovery process and to make it easier for victims to erase fraudulent items from their credit history.

PROTECTING YOURSELF:

While no crime can ever be fully prevented, there are some steps that can be taken to decrease risk:

- Check your credit reports once a year from the three major credit reporting agencies.

- Guard your Social Security number. When possible, don't carry your Social Security card with you. Don't put your SSN or drivers license number on your checks.
- Guard your personal information. You should never give your Social Security number to anyone unless they have a good reason for needing it. Watch out for eavesdroppers.
- Carefully destroy papers you throw out, especially those with sensitive or identifying information that an identity thief can find in the dumpster or the garbage.
- Be suspicious of telephone solicitors. Never provide information unless you initiated the call.
- Use a locked mailbox to send and receive all mail.
- Reduce the number of pre-approved credit card offers you receive. If you call 888-5OPT OUT, you can reduce the number of credit companies who access your credit history to send you pre-approved cards. (Please be advised that you will be asked for your SSN.)

VICTIMS OF IDENTITY THEFT SHOULD:

- Call the three credit reporting agencies and place a fraud alert on their Social Security numbers. They should get the agencies to send them copies of their reports and should look them over carefully for any fraudulent activity or inaccuracies.
- Call the police and file a complaint. They should make sure to get a copy of the police report. **(Please note that it is illegal to pretend that you are a victim of identity theft in order to get out of your debts.)**
- Call and write all the creditors who have opened fraudulent accounts and tell them that they've become a victim of ID theft. The companies must provide upon request copies of all application and transaction information on the account.

RESOURCES:

Credit Reporting Agency contact information

TransUnion: 800-888-4213, *www.tuc.com* (fraud division -- 800-680-7289)
Experian: 888-EXPERIAN, *www.experian.com* (fraud division -- 888-397-3742)
Equifax: 800-685-1111, www.equifax.com (fraud division -- 800-525-6285)

Federal Trade Commission Identity Theft Office: www.consumer.gov/idtheft or 877-IDTHEFT

Sources: Federal Trade Commission, General Accounting Office, Congressional Research Service, Gartner Inc.